## REMARKS

### Status of the Claims

- Claims 1-2, 4-5, and 7-13 are pending in the Application after entry of this amendment.
- Claims 1-13 are rejected by Examiner.
- Claim 3 is cancelled by Applicant.
- Claims 1, 5-6, 9, and 11 are amended by Applicant.

### Amendments to the Specification

The Abstract of the Specification is objected to for using the claim-like term "said". Applicant amends the Abstract to avoid the use of claim-like language.

The Specification is objected to on page 6 for referring to hyperlinks. Applicant amends the Specification to remove the hyperlinks.

Applicant respectfully requests reconsideration and withdrawal of the objections to the Specification based on the above-mentioned amendments. Applicant submits that no new matter has been added via these amendments.

### Claim Objections

Claims 1 and 5 are stand objected. Claim 5 is amended to address a preliminary amendment editing concern. Claims 1 and 5 are amended to address an antecedent basis concern. Applicant respectfully submits that the amendments overcome the objections. Withdrawal of the objections is respectfully requested.

### Claim Rejections Pursuant to 35 U.S.C. §103

Claims 1-2, 5, 7-8, 10, and 12-13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Menezes "Handbook of applied cryptography" (Menezes) in view of U.S. Patent No. 6,763,112 to Haumont (Haumont).

Claim 1 is directed to a method performed by a receiver to verify that data received by the receiver was sent by an authorized transmitter. Amended Claim 1 includes subject matter from now-cancelled Claim 3. Claim 1 reads, in relevant part:

"…(a) generating a random number; (b) broadcasting said random number and said identifier over the network;

(c) receiving from the transmitter a response computed by applying a first function to said random number and to said identifier;

(d) verifying the received response by applying a second function to the received response, to said random number and to said identifier;…"

(Part of pending Clam 1)

Menezes at paragraph 10.16, part 3, page 402, describes a method of mutual authentication that Applicant interprets as follows:

(1) a receiver (B) sending to a transmitter (A) a random number ($r_B$) generated by the receiver;

(2) a transmitter (A) sends to the receiver an encryption of the random number ($r_B$) generated by the receiver, another random number ($r_A$) generated by the transmitter, and an optional message (B*);

(3) the receiver (B) sending to the transmitter (A) an encryption of the random number ($r_B$) generated by the receiver, and random number ($r_A$) generated by the transmitter.

Applicant notes that Menezes fails to send an identifier from the receiver to the transmitter in step (1) above. Applicant notes that the identifier in Claim 1 is associated with the data sent by the transmitter. Whereas amended Claim 1 at step (b) performs "broadcasting said random number and said identifier", Menezes at step (1) only sends a random number ($r_B$) to the transmitter.

Applicant notes that Menezes generates and sends, at step (2), two random numbers ($r_A$), ($r_B$), and an optional message (B*) that is generated by the transmitter. Whereas amended Claim 1 at step (c) performs "receiving from the transmitter a response computed by applying a first function to said random number and to said identifier", Menezes fails to include any identifier associated with data in the receiver. Menezes at step (2) also includes a random number ($r_A$) and an optional message (B*) generated by the transmitter. These transmitter-generated elements of Menezes do not appear in amended Claim 1.

Applicant notes that Menezes, at step (3), generates and sends an encryption of the random number ($r_B$) generated by the receiver and random number ($r_A$) generated by the transmitter. Whereas amended Claim 1, at step (d) performs "verifying the received response by applying a second function to the received response, to said random number and to said identifier", Menezes, at step (3) does not include applying a second function to the received response, the random number and the identifier associated with data in the receiver. Menezes does not perform step (d) of amended Claim 1 because Menezes does not discuss an identifier associated with data that resides in the receiver.

Thus, Menezes fails to discuss all aspects of pending amended Claim 1; specifically, steps (b), (c), and (d) because Menezes fails to discuss a receiver sending an identifier associated with data in the receiver to a transmitter where the identifier information is processed by the transmitter and verified by the receiver. Specifically, Menzes fails to discuss broadcasting a random number and an identifier from a receiver over a network, receiving from the transmitter a response computed by applying a first function to the random number and to the identifier, and verifying the received response by applying a second function to the received response, to the random number and to the identifier as recited in pending Claim 1.

Haumont describes a security procedure for use with a mobile communication service in a mobile communication system having a core network connected to a plurality of radio access networks respectively providing radio coverage over radio

access network areas, each of the plural radio access networks having a radio network controller and a base station, said security procedure comprising the steps of: detecting, by a radio network controller a communication failure between the radio network controller and a mobile station, the radio network controller controlling radio coverage in a radio access network area in which the mobile station is located; transmitting a request from the radio network controller to the core network to perform an authentication of the mobile station; and performing a mobile station authentication procedure between the core network and the mobile station. (See Haumont, granted Claim 1).

However, Haumont, like Menezes, fails to discuss steps (b), (c), and (d) of pending Claim 1 because Haumont fails to describe broadcasting from a receiver of data, a random number and an identifier over a network, receiving from the transmitter a response computed by applying a first function to the random number and to the identifier, and verifying the received response by applying a second function to the received response, to the random number and to the identifier as is recited in pending independent Claim 1.

Applicant respectfully submits that the combination of Menezes and Haumont fails to teach or suggest the Claim 1 elements (b), (c), and (d) because each of Menezes and Haumont fails to teach these elements as discussed above.

Pending Claim 5 is directed to a method for proving that data sent to a receiver have been transmitted by a transmitter authorized by a trusted third party. Amended Claim 5 includes subject matter from now-amended Claim 6. Although drafted from the transmitter point of view, amended pending Claim 5 contains elements similar to that of pending Claim 1 and thus, for the same reasons as stated above, Claim 5 is patentably distinct compared to the cited art of Menezes and Haumont.

Since the combination of Menezes and Haumont fails to teach or suggest all aspects of amended independent Claims 1 and 5, then the combination of Menezes and Haumont cannot render obvious pending independent Claims 1 and 5 under 35 USC

§103(a) as well as their dependent Claims 2 and 7-8, 10, and 12-13 per MPEP §2143.03.

Applicant respectfully requests reconsideration and withdrawal of the 35 USC §103(a) rejections on Claims 1-2, 5, 7-8, 10, and 12-13 in light of the arguments presented above.

Claims 4, 6, 9, and 11 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Menezes "Handbook of applied cryptography" (Menezes) in view of U.S. Patent No. 6,763,112 to Haumont (Haumont), and in further view of U.S. Patent No. 5,815,665 to Teper et al. (Teper).

The teachings of Menezes and Haumont are discussed above.

Teper discusses an Online Brokering Service provides user authentication and billing services to allow users to anonymously and securely purchase online services from Service Providers (SP) sites (e.g., World Wide Web sites) over a distributed public network, which may be an untrusted public network such as the Internet. Users and SP sites initially register with the Brokering Service, and are provided with respective client and server software components for using the Brokering Service. In one embodiment, when a user initially connects to an SP site, the SP site transmits a challenge message over the public network to the user computer, and the user computer generates and returns and cryptographic response message (preferably generated using a password of the user). The SP site then passes the response message to the Brokering Service, which in-turn looks up the user's password and authenticates the response message. (See Teper, Abstract).

However, Teper, like Menezes and Haumont, also fails to describe the elements of " broadcasting said random number and said identifier over the network, receiving from the transmitter a response computed by applying a first function to said random number and to said identifier, and verifying the received response by applying a second function to the received response, to said random number and to said identifier" as recited in independent Claims 1 and 5.

As a result, Applicant respectfully submits that the combination of Menezes, Haumont, and Teper cannot render obvious independent Claims 1 and 5 and their respective dependent Claims 4, 6, 9, and 11 under 35 USC §103(a) per MPEP §2143.03.

**Conclusion**

Applicant respectfully submits that the pending claims patentably define over the cited art and respectfully requests reconsideration and withdrawal of all rejections of the pending claims. Reconsideration for a Notice of Allowance for all pending claims is respectfully requested.

If there are any additional charges in connection with this requested amendment, the Examiner is authorized to charge Deposit Account No. 07-0832 therefore.

Respectfully submitted,
Eric Diehl, et al.

Date: November 12, 2008

/Jerome G. Schaefer/

Jerome G. Schaefer
Attorney for Applicant
Registration No. 50,800
(609) 734-6451

Thomson Licensing, LLC
Patent Operation
PO Box 5312
Princeton, NJ 08543-5312